PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-107787
(43)Date of publication of application : 24.04.1998

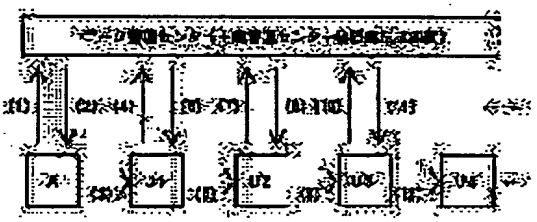
(51)Int.Cl. H04L 9/08
G06F 12/14
G06F 15/00
G09C 1/00
H04L 9/14
H04L 9/32

(21)Application number : 08-277125
(22)Date of filing : 27.09.1996

(71)Applicant : MITSUBISHI CORP
(72)Inventor : SAITO MAKOTO

(54) DATA MANAGEMENT SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To ensure security of data in a network.
SOLUTION: (1) An author A indicates a copyright label (L0) to a data management center to request the distribution of an original private key (Ks0). (2) The center encrypts the L0 and its corresponding key Ks0 with a public key (Kba) of the author A and distributes the encrypted original private key (CksOkba) to the author A. In this case the center applies undirectional hash processing to the L0 to generate a label fingerprint (D0) and distributes it to the author A. (3) The author A decodes the key (CksOkba) with a specified key of the author A and encrypts original work data (M0) with the decoded Ks0 and transfers the encrypted M0, the L0 and the F0 to a first user U1. (4) The first user U1 indicates the L0, the F0 and a 1st user label (Lu1) to the center to ask for the distribution of a 1st private key (Ks1). (5) the center confirms the user to be a legal user through the F0, registers the label Lu1 and encrypts the Ks0 and the Ks1 with the public key of the first user U1 and distributes the result to the first user U1. (6) The first user U1, decodes the encrypted keys by the specified key of the U1 and uses the Ks0 to decode the encrypted data.



LEGAL STATUS

[Date of request for examination] 26.09.2003
[Date of sending the examiner's decision of rejection] 14.09.2004
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1] It is the data management system which manages the digital data transmitted to a data user from a data owner through a communication network. In the :aforementioned data management system A private key, a public key, an exclusive key, a data owner label, a data user label, and a data label are used, and; data control center links with a public key storage engine and a private key generation engine. While it is arranged on said communication network and the; aforementioned data control center attests the public key of said data owner and said data user Are keeping said data owner label, said data user label, and said data label, and the; aforementioned data owner presents a data owner label and a data label. Require the private key for data encryption of said data control center, and the; aforementioned data control center creates a data label fingerprint from said data label. Distribute among said data owner the private key for encryption enciphered using the public key of said data label fingerprint and said data owner, and the; aforementioned data owner enciphers data using said private key decoded using said data owner's exclusive key. Transmit said encryption data, said data label, and said data label fingerprint to the first user, and the data user of the; aforementioned beginning presents said user label of the first data user, said data label, and said data label fingerprint. Require the private key for [said / which is data re-enciphered] having decoded with the private key for decoding said encryption data in said data control center, and the; aforementioned data control center checks the justification of said data label with said data label fingerprint. While registering said first data user's user label It enciphers using said first data user's public key, and the private key for [said / which is data re-enciphered] having decoded with the private key for decoding said encryption data is distributed to said first data user. The data user of the; aforementioned beginning Said private key for a decryption and said private key for re-encryption are decoded using said first data user's exclusive key. Decode encryption data using said private key for a decryption, use, and said decoded data are enciphered and copied [save and] using said private key for re-encryption. Said encryption data are transmitted to the next data user with the user label of a data label, a data label fingerprint, and the first data user.
[Claim 2] The data management system according to claim 1 with which copyright registration is performed when said data owner shows a data control center said data owner label and said data label.
[Claim 3] The data management system according to claim 1 with which processing of said data is performed by the user of data, and the contents of processing of said data are added to said data label.
[Claim 4] The data management system according to claim 3 with which secondary copyright registration is performed when said data user shows a data control center the data label with which the user label and said contents of processing of said data were indicated.
[Claim 5] The digital data managerial system of claim 3 or claim 4 said whose data are plurality.
[Claim 6] Claim 1 and claim 2 by which a digital signature is performed on said data label, claim 3, a data management system according to claim 4 or 5.
[Claim 7] Claim 1 to which accounting is performed based on said data user having shown the data control center said user label and said data label, claim 2, claim 3, claim 4, a data management system according to claim 5 or 6.

[Claim 8] The data management system according to claim 7 to which said accounting is performed by the operating-experience meter ring reversionary method.
[Claim 9] The data management system according to claim 8 with which said operating-experience meter ring data are kept in the data control center.
[Claim 10] The data management system according to claim 8 with which said operating-experience meter ring data are kept by a user's equipment.
[Claim 11] The data management system according to claim 7 to which said accounting is performed by the prepayment method.
[Claim 12] The data management system according to claim 11 with which the data of said prepayment are kept in the data control center.
[Claim 13] The data management system according to claim 11 with which the data of said prepayment are kept by a user's equipment.
[Claim 14] Claim 1 as which said digital data has the usual file structure, and only the data body is enciphered, claim 2, claim 3, claim 4, claim 5, claim 6, claim 7, claim 8, claim 9, claim 10, claim 11, a data management system according to claim 12 or 13.
[Claim 15] The data management system according to claim 14 with which said some of data bodies are enciphered.
[Claim 16] The data management system according to claim 15 with which said some of data bodies are enciphered continuously.
[Claim 17] The data management system according to claim 15 with which said some of data bodies are enciphered by discontinuity.
[Claim 18] Claim 1 as which said digital data has the usual file structure, and a data header and the data body are enciphered, claim 2, claim 3, claim 4, claim 5, claim 6, claim 7, claim 8, claim 9, claim 10, claim 11, a data management system according to claim 12 or 13.
[Claim 19] The data management system according to claim 18 with which said a part of data header and all of said data bodies are enciphered.
[Claim 20] The data management system according to claim 18 with which said a part of data header and some data bodies are enciphered.
[Claim 21] Claim 1 as which said digital data has the usual file structure, and only the data header is enciphered, claim 2, claim 3, claim 4, claim 5, claim 6, claim 7, claim 8, claim 9, claim 10, claim 11, a data management system according to claim 12 or 13.
[Claim 22] The data management system according to claim 21 with which all of said data headers are enciphered.
[Claim 23] The data management system according to claim 21 with which said a part of data header is enciphered.
[Claim 24] Claim 1 as which said digital data has the usual file structure, and only the copyright label is enciphered, claim 2, claim 3, claim 4, claim 5, claim 6, claim 7, claim 8, claim 9, claim 10, claim 11, a data management system according to claim 12 or 13.
[Claim 25] The data management system according to claim 24 with which said some of copyright labels are enciphered.
[Claim 26] Claim 1 as which said digital data has the file structure of an object format, and the method is enciphered, claim 2, claim 3, claim 4, claim 5, claim 6, claim 7, claim 8, claim 9, claim 10, claim 11, a data management system according to claim 12 or 13.
[Claim 27] It is the system which manages the digital data transmitted to a data user from a data owner through broadcast, a communication network, or a data accumulation medium. In this data management system A public key, an exclusive key, a data user label, and a data label are used, and; data control center and a data owner link with a public key storage engine. While it is arranged on said communication network and the; aforementioned data control center attests the public key of said data owner and said data user Said data user label and said data label are kept, the data user of; beginning presents a data user label, and receives and uses data and a data label from the inside of said network, and said data are not saved in said data user's equipment after use termination.
[Claim 28] The data management system according to claim 27 which is not saved in said data user's equipment by eliminating said data.
[Claim 29] The data management system according to claim 27 which is not saved in said data user's equipment by forming said data into an one direction hash value.

[Claim 30] The data management system according to claim 27 which said data control center links further with the private key generation engine, and said data are enciphered using a private key, and is saved in said data user's equipment.
[Claim 31] Claim 28 from which processing of data is performed and a processing label is obtained by adding the contents of processing of data to said data label, a data management system according to claim 29 or 30.
[Claim 32] The data management system according to claim 31 with which only said processing label is transmitted to the next data user.
[Claim 33] Said next data user decodes said encryption processing label using said next data user's exclusive key. said processing label is enciphered using said next user's public key, and it transmits to said next data user — having —; — said decoded processing label — said data control center — showing —; — said data control center — said processing label — being based — data — said next data user — transmitting —; — said next user processes data with the processing data of said processing label, and uses — A data management system according to claim 32.
[Claim 34] said first user — said processing data — said next user — transmitting —; — said next data user — said next data user — said processing data — said data control center — showing —; — said data control center — said processing label — being based — data — said next data user — transmitting —; — the data management system of claim 32 which said next user processes data with the processing data of said processing label, and uses.
[Claim 35] The data management system according to claim 34 with which said first user performs a digital signature on said processing label using said first user's exclusive key.
[Claim 36] Claim 28 and claim 29 whose data are plurality, claim 30, claim 31, claim 32, claim 33, a digital data managerial system according to claim 34 or 35.
[Claim 37] Claim 27 to which accounting is performed based on said data user having shown the data control center said user label and said data label, claim 28, claim 29, claim 30, claim 31, claim 32, claim 33, claim 34, a data management system according to claim 35 or 36.
[Claim 38] The data management system according to claim 37 to which said accounting is performed by the operating-experience meter ring reversionary method.
[Claim 39] The data management system according to claim 38 with which said operating-experience meter ring data are kept in the data control center.
[Claim 40] The data management system according to claim 38 with which said operating-experience meter ring data are kept by a user's equipment.
[Claim 41] The data management system according to claim 37 to which said accounting is performed by the prepayment method.
[Claim 42] The data management system according to claim 41 with which the data of said prepayment are kept in the data control center.
[Claim 43] The data management system according to claim 41 with which the data of said prepayment are kept by a user's equipment.
[Claim 44] Claim 28 as which said digital data has the usual file structure, and only the data body is enciphered, claim 29, claim 30, claim 31, claim 32, claim 33, claim 34, claim 35, claim 36, claim 37, claim 38, claim 39, claim 40, claim 41, a data management system according to claim 42 or 43.
[Claim 45] The data management system according to claim 44 with which said some of data bodies are enciphered.
[Claim 46] The data management system according to claim 45 with which said some of data bodies are enciphered continuously.
[Claim 47] The data management system according to claim 45 with which said some of data bodies are enciphered by discontinuity.
[Claim 48] Claim 28 claim 29 as which said digital data has the usual file structure, and a data header and the data body are enciphered, claim 30, claim 31, claim 32, claim 33, claim 34, claim 35, claim 36, claim 37, claim 38, claim 39, claim 40, claim 41, a data management system according to claim 42 or 43.
[Claim 49] The data management system according to claim 48 with which said a part of data header and all of said data bodies are enciphered.
[Claim 50] The data management system according to claim 48 with which said a part of data

header and some data bodies are enciphered.
[Claim 51] Claim 28 claim 29 as which said digital data has the usual file structure, and only the data header is enciphered, claim 30, claim 31, claim 32, claim 33, claim 34, claim 35, claim 36, claim 37, claim 38, claim 39, claim 40, claim 41, a data management system according to claim 42 or 43.
[Claim 52] The data management system according to claim 51 with which all of said data headers are enciphered.
[Claim 53] The data management system according to claim 51 with which said a part of data header is enciphered.
[Claim 54] Claim 27 as which said digital data has the usual file structure, and only the copyright label is enciphered, claim 28 claim 29, claim 30, claim 31, claim 32, claim 33, claim 34, claim 35, claim 36, claim 37, claim 38, claim 39, claim 40, claim 41, a data management system according to claim 42 or 43.
[Claim 55] The data management system according to claim 54 with which said some of copyright labels are enciphered.
[Claim 56] Claim 27 as which said digital data has the file structure of an object format, and the method is enciphered, claim 28 claim 29, claim 30, claim 31, claim 32, claim 33, claim 34, claim 35, claim 36, claim 37, claim 38, claim 39, claim 40, a data management system according to claim 41, 42, or 43.
[Claim 57] It is the quotient trading system performed through a broker between a need person and a producer. In :this quotient trading system A private key and the key only for public key – are used, and the; aforementioned broker links with a public key storage engine and a private key generation engine. It is arranged on a communication network, the; aforementioned need person makes demands on said broker for commercial transaction data, and the; aforementioned broker with the private key for encryption enciphered using the public key of the person from Norio Saki Transmit a commercial transaction data demand of said need person to the person from Norio Saki, and the; aforementioned producer decodes said private key for encryption using the exclusive key of the person from Norio Saki. Encipher said commercial transaction data using said decoded private key for encryption, send to said broker, and the; aforementioned broker decodes said encryption commercial transaction data using said private key for encryption. Transmit said decoded commercial transaction data to said need person with said private key for re–encryption which re–enciphered using the private key for re–encryption, and was enciphered using said need person's public key, and the; aforementioned need person decodes said private key for re–encryption using said need person's exclusive key. Said encryption commercial transaction data are decoded using said decoded private key for re–encryption. Write down an order matter in said decoded commercial transaction data, and a purchase order is drawn up. Encipher said purchase order using said private key for re–encryption, send said re–encryption purchase order to said broker, and the; aforementioned broker decodes said re–encryption purchase order using said private key for re–encryption. Said decoded purchase order is enciphered using the public key of the person from Norio Saki, said encryption purchase order is transmitted to the person from Norio Saki, and the; aforementioned producer decodes said encryption purchase order using the exclusive key of the person from Norio Saki, and performs order–received processing.
[Claim 58] The data management system according to claim 57 with which said digital data has the usual file structure, and only the data body is enciphered.
[Claim 59] The data management system according to claim 58 with which said some of data bodies are enciphered.
[Claim 60] The data management system according to claim 59 with which said some of data bodies are enciphered continuously.
[Claim 61] The data management system according to claim 59 with which said some of data bodies are enciphered by discontinuity.
[Claim 62] The data management system according to claim 57 with which said digital data has the usual file structure, and a data header and the data body are enciphered.
[Claim 63] The data management system according to claim 62 with which said a part of data header and all of said data bodies are enciphered.
[Claim 64] The data management system according to claim 62 with which said a part of data

header and some data bodies are enciphered.
[Claim 65] The data management system according to claim 57 with which said digital data has the usual file structure, and only the data header is enciphered.
[Claim 66] The data management system according to claim 65 with which all of said data headers are enciphered.
[Claim 67] The data management system according to claim 65 with which said a part of data header is enciphered.
[Claim 68] The data management system according to claim 57 with which said digital data has the usual file structure, and only the copyright label is enciphered.
[Claim 69] The data management system according to claim 68 with which said some of copyright labels are enciphered.
[Claim 70] The data management system according to claim 57 with which said digital data has the file structure of an object format, and the method is enciphered.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the digital data managerial system applied effective in management of digital data especially copyright management of work data, electronic commerce, and electronic money.
[0002]
[Description of the Prior Art] The database system which uses mutually various kinds of data which each computer saved independently by connecting each computer by the communication line until now today when it is called the information age is spreading. coding information with little amount of information which can process the information which set to this database system and has been treated by until by classic computer — and it was monochrome binary data like facsimile information in ** and time at most, and amount of information like natural drawing and an animation could not be markedly alike, and was not able to deal with many data.
[0003] While the digital processing technique of various electrical signals develops, development of a digital processing technique is conventionally furthered also for picture signals other than the binary data currently treated only as an analog signal. Since it becomes possible to treat a picture signal like a television signal by computer by digitization of this picture signal, the "multi-media system" which deals with the data of the various kinds which a computer treats, and the image data which digitized the picture signal to coincidence attracts attention as a future technique.
[0004] Since there is much amount of information, if image data remains as it is overwhelmingly as compared with alphabetic data and voice data, preservation, a transfer, or various kinds of processings in a computer are difficult for it. Therefore, it was possible to compress / elongate these image data, and the specification image data compression / for some elongation has been created. In it, MPEG 2 specification corresponding to high definition television broadcasting was created as common specification until now from JPEG (Joint Photographic image coding ExpertsGroup) specification for static images, H.261 specification for a television meeting, MPEG1 (Moving Picture image coding Experts Group 1) specification for image storage, and current television broadcasting. With these techniques, the real-time operation of digital image data is becoming possible.
[0005] Since quality deteriorated whenever the analog data which has spread widely conventionally carries out preservation, a copy, processing, and a transfer, processing of the copyright produced according to these activities did not become a big problem. However, since quality degradation does not produce digital data even if it repeats preservation, a copy, processing, and a transfer and performs them, processing of the copyright produced according to these activities is a big problem. Until now, there is no exact approach in copyright processing of digital data, and it is the Copyright Act, or is processed by the contract, and the compensation to sound recording / image transcription device of a digital method is institutionalized also in the Copyright Act.
[0006] the directions of a database are online via a communication line about the data used effectively and processed by it not only referring to the contents, but saving, copying and processing the usually obtained data — it is — it is even possible to transmit to others, or to transmit to a database using a suitable storage, further on-line, and to register as new data.

Although only alphabetic data had been applicable in the conventional database system, in a multi-media system, in addition to data, such as an alphabetic character put in a database until now, the voice data and the image data which are originally analog data are digitized, and it considers as a database.

[0007] In such a situation, although how the copyright of the data put in a database is dealt with poses a big problem, the copyright management tool for it and especially the copyright management tool completed about secondary use of a copy, processing, a transfer, etc. are not the place which is the former.

[0008] The computer communication system which is the data communication using the computer currently performed on a scale of being on the other hand until now comparatively small, and has been called the Internet in the past several years spreads quickly, and is becoming a familiar existence for all people. Although the information which communicates by this Internet system was only text at the beginning, according to progress of a technique, voice data and image data are going to be dealt with, and even electronic commerce data with still more important dependability and secret nature or electronic money data is going to be dealt with by the Internet system.

[0009] The need for establishment of an accounting technique when thus, the assurance technology of the safety about the secret nature of the data dealt with and dependability and accounting are required is demanded.

[0010] Although the opinion of copyright is made about the work data charged to use in many cases, there are some work data which do not assert copyrights, such as individual mail, an advertisement, and advertisement, positively. For example, in the individual mail without the opinion of copyright, reservation of privacy, contents alteration prevention, and forged prevention are important. Moreover, even if it is data for an advertisement / advertisement which do not usually assert copyright, generating of the damage by the alteration of the contents, distribution to a non-candidate, or derangement of the business by fake data may occur. Thus, if it is in individual mail, alteration prevention of the contents, invasion-of-privacy prevention, and forged prevention are required, and if it is in advertisement / advertisement data, alteration prevention of the contents, a perusal limit, and forged prevention are required.

[0011] Invasion-of-privacy prevention of individual mail and a perusal limit of advertising advertisement data can realize by the data encryption, and alteration prevention of individual mail and advertising advertisement data forged prevention, individual mail and advertisement / advertisement data is realized by check (authentication) of an addresser.

[0012] The security of the system itself of the Internet system which has the grass-roots-way of thinking is very brittle. The system for securing the security of the Internet system is proposed, and there are PEM (Privacy Enhanced Mail) which takes a layered structure as a typical system, and PGP (Pretty Good Privacy) which takes horizontal dispersion structure. Although each of these performs the confidential nature of data, authentication of a sending agency, non-altered certification of data, the first addresser's display, and management of a public key, each limit of reuse including processing of data is impossible.

[0013] With the top engine called IPRA (Internet PCA Registration Authority) in PEM which takes a layered structure It organizes with the engine like a degree called PCA (Policy Certification Authority) (Organizational). It consists of lowest engines respectively called an area (Regidential) and an individual (Personal). Guarantee engine of a high order (Certifucation Authorityies) The justification of the public key is guaranteed by publishing the public key certificate which carried out the digital signature to data, such as a low-ranking engine's name, about a low-ranking engine's public key.

[0014] At PGP which takes horizontal dispersion structure, it is Certifucation Authority of PEM. A corresponding engine guarantees the justification of the public key, when there is nothing and others who can trust it publish the public key certificate which carried out the digital signature to data, such as a name of a public key. There is the approach of calling the electronic fingerprint which checks with voice the hash value of 16 bytes which hashed the public key with one direction hash (hash) functions, such as MD5 (Message Digest 5), as a simple symptom of a public key in this PGP.

[0015] Although there is no problem about an authentication person at PEM which takes a

layered structure when PEM is compared with PGP, it cannot necessarily be said in the grass roots Internet system that it is a common system. On the other hand, although it is a large employable system that PGP is simple and generally, when the signer who can trust it is not found, it cannot use.

[0016] By the way, each computer currently used by the stand-alone is conventionally connected through a network system with development of a computer network system, the database system which shares data spreads, and not only data but an application program and the distributed object system shared through a network to the basic software further called an operating system are proposed.

[0017] A distributed object system is supplied from a server as an object which both data and software become from a program and data. A server provides a distributed object system with an operating system, an application program, and data, a server provides it with the system called the object container which performs data processing and data storage with the user-terminal equipment which is the usual computer, an operating system, an application program, and data, and although the user-terminal equipment called a network computer performs data processing, there is a system called the server object server to which a server performs preservation of data. This server object server system is pushed further, a server also performs data processing, user-terminal equipment has only the function of I/O, but even what the whole system functions on as one computer is considered.

[0018] Moreover, the entrepreneur who offers network bases, such as a communication line, offers accounting systems other than a communication line, a security system, a copyright managerial system, an authentication system, etc. as another gestalt of a network system, and it conceives of the "lease network system" called the license network where a service entrepreneur does like a self system using such system services, and undertakes a network business.

[0019]

[Summary of the Invention] An artificer proposes the digital data managerial system for realizing safety reservation of the digital data protection of copyrights in a computer network system, a usual distributed object system, and a usual license network system, and electronic commerce data, and safety reservation of electronic money data in this application.

[0020] The 1st digital data managerial system consists of the original copyright person or information provider using the data control center and network on a network, and two or more users. A data control center grasps the data use situation by the demand of a private key while distributing the data encryption private key to authentication and user label presentation of a network user's public key. Although it is enciphered using a private key and data are saved and transmitted, preservation and the data to transmit are enciphered with a different private key from the private key of the transmitted data. Moreover, a original data label is added to original data, a processing data label is added to processing data, and a data control center does not perform storage of data, but performs only storage of a original data label and processing data. Although a user label is used for the demand of a private key, the electronic fingerprint of a user label can also be used instead.

[0021] The 2nd digital data managerial system consists of two or more users using the data control center, the original copyright person or information provider, and network on a network. A data control center performs storage of a user label Hara data label and a processing data label while performing storage of authentication and original data of a network user's public key, and a processing scenario. Among users, data are not transmitted but the data label enciphered with the public key is transmitted. Although a data label is used for a transfer and a use application, the electronic fingerprint of a data label can also be used instead.

[0022] In an electronic commerce system, all data circulate through the broker on a network, the data transmitted to a need person from a producer are enciphered with the private key for encryption, and the data transmitted to a producer from a need person are enciphered with the private key for re-encryption.

[0023]

[Example] As an example of this invention, although the 1st example – the 5th example are explained, the fundamental matter common to these examples is explained first.

The engine for attesting the copyright person of original paper crops, the provider (Information Provider:IP) of original paper crops, the user of original paper crops, and the processing person of original paper crops is required of [certificate authority] this invention. Although this engine may be the only thing, two or more engines may exist. Two or more engines can make it possible to consider that he is one engine virtually by making them link to an existence case.
[0024] Moreover, in this system, a different private key for every phase with which the set and work of the key only for public key – of each user are used is used. In these, an exclusive key secures dependability, when a certificate authority performs a digital signature to the public key with which each user manages and corresponds in his responsibility. Although the key management engine called a key library generally manages this public key and it is distributed according to a demand of a user, the engine which is made to link the engine which has an authentication function with a key management engine, or has an authentication function can have a key management engine's function.
[0025] The key system and digital signature system by which [cryptographic key] use is carried out are explained briefly. Since encryption and a decryption are also called a "common key system" with the same key for a ****** reason and need to make a key secret, a private key (secret key) system is called a "private key system." The DES (Data Encryption Standard) system of NBS (National Bureau of Standards), the FEAL (Fast Encryption Algorithm) system of Nippon Telegraph and Telephone, and the MISTY system of Mitsubishi Electric are typical as cryptographic algorithm using a private key. In the example explained below, a private key is displayed as "Ks."
[0026] On the other hand, using the exclusive key (priVate key) made secret in addition to the owner of the public key (puBlic key) currently exhibited and its key, a public key system is a code system which enciphers with one key and is decrypted with the key of another side, and a RSA public key system is typical. In the example explained below, an exclusive key is displayed for a public key as "Kv" with "Kb." It is the actuation which enciphers Data M (Material) to the code Ck (Cryptgram) which used the cryptographic key K at this time (Encryption) Ck=E (M, K) It is the actuation which decrypts Code Ck to Data M using a cryptographic key K (Decryption) M=D (Ck, K)
It expresses.
[0027] A digital signature is a technique adapting a public key system, and the source makes Data M a hash value Hm by one-way hash functions, such as MD5. Encipher the hash value Hm to Chmkv using the exclusive key Kv, and it transmits to the destination with Data M. The destination makes the data M transmitted while decrypting transmitted encryption hash value Chmkv to the hash value Hm using the public key Kb hash value Hm' by the same one-way hash function. If it is Hm=Hm', it is the system judged as the transmitted data being reliable. In addition, it is impossible for the hash value Hm obtained in this process to be calculated in 1 mind from Data M, and to reproduce Data M in 1 mind from a hash value Hm. Moreover, even if it is the case where it transmits without enciphering a hash value Hm when the source and the destination can check mutual, since the dependability of transfer data is secured, it is called an electronic fingerprint (electronic fingerprinting) and used for simple authentication.
[0028] Although a data encryption / decryption / re-encryption processing, preservation prohibition processing of data, and storage of a cryptographic key are performed in equipments other than center side equipment in the 1st example of [use of a key] – the 5th example, the application program of the dedication which operates automatically, the application program built in data, or in order to make safety high more, as for these actuation, to be performed by the operating system is desirable. Moreover, more advanced safety can be obtained by performing these processings using an IC card or a PC card.
[0029] There are an approach of performing accounting according to the use hope before use as an approach of ensuring accounting according to use of [accounting] data, and a method of performing accounting according to an operating experience after use. Moreover, the operating experience is recorded on the approach of charging after use, and there are a meter ring reversionary method which investigates use record and charges it later, and a card prepayment method with which the entry amount of money is reduced according to an operating experience using the card in which the purchase amount of money was entered beforehand in it.

Furthermore, there are a telephone rate method with which the recording apparatus is installed in the server side, and an electricity bill method with which the recording apparatus is installed in the user-terminal equipment side as meter ring reversionary method. Moreover, there are a credit card method with which the prepaid card is kept by the card prepayment method at the server side, and a prepaid card method with which the prepaid card is kept at the user side.
[0030] In the 1st example - the 4th example, based on User Information shown when registering that a user uses a system, a data control center creates a user label, it transmits to a user, and the user keeps the user public key used in a user label and a system, the key only for users, and the public key of a data control center in his equipment. As these storage areas, although an IC card or a PC card is the optimal, it can also be kept in the data storage equipment in equipment. The cryptographic key storage approach by the IC card or the PC card can secure safety higher than the key management by the operating system.
[0031] Although the example explained below explains the system which manages digital data copyright, it has the digital data of which secrecy nature, certainty, and dependability, such as the contents of a communication link, such as electronic commerce data and electronic money data, and the contents of dealings, are required besides work data, and can apply this invention also to these digital data. Moreover, although the engine which generates the engine and cryptographic key which keep a cryptographic key in the network system which uses a cryptographic key is placed out of a network system and it is used via a network system, in the example explained below, it explains serving as the only engine, i.e., a data control center, and the engine of all ********, in order to simplify explanation.
[0032] By [label] this invention, since a label is used in order to protect the copyright of data and to use data copyright, drawing 1 , drawing 2 , and drawing 3 are first used and explained about a label. In this system, although a system user's user label is used, as shown in drawing 1 (a), a label owner's information is indicated by the user label. When a label owner furthermore has original copyright, as it is shown in drawing 1 (b), the information about original paper crops is added. In being the processing work with which the work processed original paper crops, and was obtained, as it shows in drawing 1 (c), the information about original copyright data, the information on a processing tool, and processing data (processing scenario) are added further. As shown in drawing 1 (d), a processing tool (processing program) can also be added instead of processing tool information. The label with which the "copyright label", the call, and the processing scenario further shown in drawing 1 (c) and drawing 1 (d) were indicated in the label with which the information on the work shown in a "user label", a call, and drawing 1 (b) in the label with which only a label owner's information shown in drawing 1 (a) was indicated was indicated is called a "processing label" among these labels.
[0033] A user label is generated by the data control center based on a user's information, when a user joins a system. A copyright label is generated by the data control center when the author who wrote a book shows a data control center the contents. A processing label is created by the data control center when the user who processed data shows a data control center a user label and a processing scenario, and these are saved in a data control center while they are transmitted to each label owner.
[0034] The relation between a copyright label and work data is shown in [object of encryption] drawing 2 (a), drawing 2 (b), and drawing 2 (c). As it was indicated in drawing 2 (b) as the case where it is separated from the header of work data as shown in drawing 2 (a), and it was indicated in drawing 2 (c) as the case where the header of work data is being unified, the copyright label may have combined with the header the work data with which a copyright label and a label correspond. When the copyright label has combined with the header, the extended label configuration which put two or more copyright labels together as shown in drawing 2 (d) can be performed. If the number of labels increases too much similarly when the extended label configuration which combined two or more labels which may be unable to contain a label to the single header which in the case of the unified label which was shown in drawing 2 (b) has a limit in capacity when a copyright label becomes large, and were shown in drawing 2 (d) is taken, a magnitude limit of the packet on the Internet may exceed, and circulation may become difficult.
[0035] A copyright label may be used without being enciphered as it was indicated in drawing 3 (b) as the case where it is enciphered and used as shown in drawing 3 (a). It is the part as

which 4 rectangular flask parts are enciphered in these drawings. In addition, work data are enciphered when a copyright label is not enciphered. In the extended label configuration shown in drawing 2 (d) even if it was the case where a copyright label was not enciphered As copyright labels other than the copyright label added at the end were enciphered and it was shown in drawing 3 (c) and drawing 3 (d) The multistage configuration in which the cryptographic key of the copyright label added and enciphered before that is contained in the copyright label added later can be adopted, and the contents of the copyright label before added by this configuration can be checked.

[0036] Although a data encryption/decryption is performed for protection of copyrights, encryption/decryption is activities with a quite large burden for a computer. Although the activity burden of encryption/decryption is not like it, either, when the data set as the object of encryption/decryption are the text data which made the alphabetic character the subject, the rating of encryption/decryption in case the target data are a video data also in voice data and image data will become huge. Therefore, even when high-speed cryptographic algorithm is used, it is not practical at a present stage to encipher / decrypt with the personal computer currently generally used except for the case where special computers, such as a super parallel mold supercomputer, are used on real time, the data, for example, the dynamic-image data, other than text data.

[0037] Drawing 4 (a), drawing 4 (b), drawing 4 (c), drawing 4 (d), drawing 4 (e), drawing 4 (f), and drawing 4 (g) explain a data encryption / decryption configuration. It is the part as which the part of four rectangular flasks is enciphered in these drawings. It is the usage of a theoretic code which was shown in drawing 4 (a), only the large data body section is overwhelmingly enciphered as compared with the head section, and the data header unit used in order to recognize data does not coincide. In such a configuration, the activity burden of encryption/decryption becomes very large.

[0038] On the other hand, as shown in drawing 4 (b), the data body section has the approach which does not encipher but enciphers a data header unit. In this case, since it becomes impossible to recognize data to encipher all headers, a part of header is not enciphered.

[0039] The data body enciphered as shown in drawing 4 (c) as an approach for mitigating the activity burden of a configuration of having been shown in drawing 4 (a) can be used only as the head part. According to this configuration, since it is only **** of the data body part that it is necessary encryption/to decrypt, the activity burden of encryption/decryption is mitigated remarkably.

[0040] Having been shown in drawing 4 (d) prepares two or more encryption sections in the data body into the data body, as the effectiveness by the configuration of drawing 4 (c) becomes higher.

[0041] What was shown in drawing 4 (e) is an approach called SKIP (Simple Key-management for Internet Protcols), while the data body was enciphered, a part of header was enciphered, and the cryptographic key for data body decode has set it into the encryption part in a header. According to this configuration, decryption is remarkably difficult in order to have to decode two codes.

[0042] However, since the whole data body section is enciphered in a configuration of having been shown in drawing 4 (e), the activity burden of encryption/decryption is very large like the case of a configuration of having been shown in drawing 4 (e). If the data body enciphered as correspondence to this by the configuration shown in drawing 4 (e) combining the configuration shown in drawing 4 (c) is used only as the head part and constituted like drawing 4 (f), since it is only **** of the data body part that it is necessary encryption/to decrypt, the activity burden of encryption/decryption will be mitigated remarkably.

[0043] In the configuration shown in drawing 4 (e), as was shown in drawing 4 (g) combining the configuration further shown in drawing 4 (d), effectiveness becomes more highly by considering as the configuration which prepared two or more encryption sections in the data body into the data body.

[0044] The data encryption / decryption configuration which has the usual file format by drawing 5 (a), drawing 5 (b), and drawing 5 (c) are explained. It is the part as which the part of four rectangular flasks is enciphered in these drawings. The data which have the usual file

format consist of the data body section and a data header unit, and consist of copyright labels which are further attached or are related in this invention. It is the usage of a theoretic code which was shown in drawing 5 (a), and it does not coincide, but only the data body section is enciphered, and a copyright label and a data header unit have the very large activity burden of encryption/decryption like the case where it is drawing 4 (a).
[0045] On the other hand, as shown in drawing 5 (b), the data body section has the approach which does not encipher but enciphers a data header unit. In this case, since it becomes impossible to recognize data to encipher all headers, a part of header is not enciphered. In addition, a copyright label is not enciphered in this case, either.
[0046] Moreover, as shown in drawing 5 (c), the data body section and a data header unit have the approach which does not encipher but enciphers a copyright label. In addition, since the relation between a copyright label and corresponding data will become unknown if all copyright labels are enciphered also in this case, some copyright labels are not enciphered.
[0047] There is "object oriented programming (object oriented programing)" which performs various processings using the "object" with which the data header and the program which treats data and data instead of the file of the usual format which consists of the data bodies were united on the other hand. The object has the underlying concept structure shown in drawing 6 (a). The data called an instance variable (instance variable) to the storing part called the slot (slot) in the container (envelope) called an instance (instance) are stored. The perimeter of a slot is surrounded in the procedure called one piece or two or more methods (method) the object for reference (refering), the object for processing (processing), for association (binding), etc. It can perform referring to or operating an instance variable only through a method, but this function is called concealment (encapsulation). Moreover, the instruction from the outside which makes reference or actuation of an instance variable perform in a method is called a message.
[0048] If this changes a view, and a method is not minded, the instance variable which cannot be referred to or operated will be protected by the method. This is used, and if it is not the message which enciphers a method and can decode the enciphered method as shown in drawing 6 (b), it can avoid referring to or operating an instance variable. Since it becomes impossible to use an object when all the methods are enciphered like the case of the data which have the usual file format shown in drawing 5 (c) also in this case, a part of method is not enciphered. In addition, it is the part as which the part of four rectangular flasks was enciphered.
[0049] [1st example] drawing 7 explains the 1st example. Although the case where it transmits to the next user is explained without a user processing original paper crop data in order to give theoretic explanation, the case where a user processes original paper crop data is explained later. In addition, the case where processing of original paper crop data is not performed in fact, and the case where processing of the original paper crop data explained in the 3rd example shown later is performed are put together and carried out. In addition, in the system of this example, a private key and the key only for public key – are used. Therefore, a public key management engine and a private key generation engine may be linked or contained in the data control center.
[0050] (1) The original paper author (data owner) A presents the original copyright label L0, and demands distribution of the original private key Ks0 of the data control center Cd. In addition, the original paper author transfers or deposits [management] original paper crop data at an information provider (IP) or a database, and an information provider (IP) or a database can play the original paper author's role. Moreover, although it is also possible to encipher the original paper crop data M0, without the original paper author's A keeping the original private key Ks0, and being dependent on the data control center Cd, in order to use the original paper crop data M0 by the user (data user), the original private key Ks0 needs to be kept in the data control center Cd.
[0051] (2) The data control center Cd of which distribution of the original private key Ks0 was required enciphers the original private key Ks0 to which the original copyright label L0 was made equivalent using the original paper author's A public key Kba with the original copyright label L0, and is Cds0 kba=E (Ks0, Kba).

Encryption Hara private key Cks0kba is distributed among the original paper author A. Henceforth, using the public key of a distribution place, it is enciphered and a private key is distributed so that it can decode only at a distribution place.
[0052] Algorithms, such as MD5 (Message Digest 5), are used for the data control center Cd for the original copyright label L0 at this time, it performs an one direction hash at it, creates ** which has 16 bytes of the original copyright label fingerprint F0, for example, amount of data, and distributes it to the original paper author A. Henceforth, this electronic fingerprint is transmitted with work data.
[0053] (3) The original paper author A among whom encryption Hara private key Cks0kba was distributed decodes encryption Hara private key Cks0kba using the original paper author's A exclusive key Kva, and is Ks0=D (Cks0 kba, Kva).
The original paper crop data M0 are enciphered using the decoded original private key Ks0, and it is Cm0ks0=E (M0, Ks0).
Encryption original paper crop data Cm0ks0, the original copyright label L0, and the original copyright label fingerprint F0 are transmitted to the 1st user (the first data user) U1.
[0054] (4) The 1st user U1 to whom encryption original paper crop data Cm0ks0, the original copyright label L0, and the original copyright label fingerprint F0 were transmitted presents the original copyright label L0, the original copyright label fingerprint F0, and the 1st user label Lu1, and demands distribution of the original private key Ks0 and the 1st private key Ks1 of the data control center Cd.
[0055] (5) The data control center Cd of which distribution of the original private key Ks0 and the 1st private key Ks1 was required While checking the justification of the shown original copyright label L0 with the original copyright label fingerprint F0 and registering the 1st user label Lu1 The 1st private key Ks1 made to correspond to the original private key Ks0 and the 1st user label Lu1 corresponding to the original copyright label L0 is enciphered using the 1st user's U1 public key Kb1, and it is Cks0kb1=E (Ks0, Kb1).
Cks1kb1=E(Ks1,Kb1)
Encryption Hara private key Cks0kb1 and 1st private key Cksof encryption1kb1 are distributed to the 1st user U1.
[0056] (6) The 1st user U1 to whom encryption Hara private key Cks0kb1 and 1st private key Cksof encryption1kb1 were distributed decodes encryption Hara private key Ck0kb1 and 1st private key Cksof encryption1kb1 using the 1st user's U1 exclusive key Kv1, and is Ks0=D (Cks0 kb1, Kv1).
Ks1=D(Cks1kb1,Kv1)
Encryption original paper crop data Cm0ks0 is decoded using the decoded original private key Ks0, and it is M0=D (M0, Ks0).
The decoded original paper crop data M0 are used.
[0057] It enciphers using the 1st private key Ks1 decoded when the original paper crop data M0 were saved and copied, and is Cm0ks1=E (M0, Ks1).
In saving and copying as encryption original paper crop data Cm0ks1 and transmitting the original paper crop data M0 to the 2nd user (the next data user) U2, it enciphers using the 1st decoded private key Ks1, and transmits as encryption original paper crop data Cm0ks1 with the original copyright label L0, the original copyright label fingerprint F0, and the 1st user label Lu1.
[0058] In addition, the digital signature of the label which enciphered the tropism hash value using a user's exclusive key on the other hand can be attached to the user's label which each user shows to the data control center Cd, a data control center can decode an encryption one side tropism hash value using the user's public key, and justification of each user label can be verified by [of the label] calculating a tropism hash value on the other hand, and comparing both the 1 directivity hash value.
[0059] (7) The 2nd user U2 to whom encryption original paper crop data Cm0ks1, the original copyright label L0, the original copyright label fingerprint F0, and the 1st user label Lu1 were transmitted presents the original copyright label L0, the original copyright label fingerprint F0, the 1st user label Lu1, and the 2nd user label Lu2, and demands distribution of the 1st private key Ks1 and the 2nd private key Ks2 of the data control center Cd.
[0060] (8) The data control center Cd of which distribution of the 1st private key Ks1 and the

2nd private key Ks2 was required checks the justification of the original copyright label L0 and the 1st user label Lu1 with the original copyright label fingerprint F0. When it is checked that the 1st user label Lu1 is just, the data control center Cd registers the 2nd user label Lu2, enciphers respectively the 2nd private key Ks2 made to correspond to the 1st private key Ks1 and the 2nd user label Lu2 corresponding to the 1st user label Lu1 using the 2nd user's public key Kb2, and is Cks1kb2=E (Ks1, Kb2).

Cks2kb2=E(Ks2,Kb2)

1st private key Cksof encryption1kb2 and 2nd private key Cksof encryption2kb2 are distributed among the 2nd user U2.

[0061] (9) The 2nd user U2 among whom 1st private key Cksof encryption1kb2 and 2nd private key Cksof encryption2kb2 were distributed decodes 1st private key Cksof encryption1kb2, and 2nd private key Cksof encryption2kb2 using the 2nd user's U2 exclusive key Kv2, and is Ks1=D (Cks1 kb2, Kv2).

Ks2=D(Cks2kb2,Kv2)

Encryption original paper crop data Cm0ks1 is decoded using the 1st decoded private key Ks1, and it is M0=D (Cm0 ks1, Ks1).

The decoded original paper crop data M0 are used.

[0062] In saving and copying the original paper crop data M0 In enciphering using the 2nd decoded private key Ks2, saving and copying encryption original paper crop data Cm0ks2 and transmitting the original paper crop data M0 to the 3rd user U3 It enciphers using the 2nd decoded private key Ks2, and encryption original paper crop data Cm0ks2 is transmitted to the 3rd user U3 with the original copyright label L0, the original copyright label fingerprint F0, the 1st user label Lu1, and the 2nd user label Lu2.

[0063] (10) The 3rd user U3 to whom encryption original paper crop data Cm0ks2 was transmitted with the original copyright label L0, the original copyright label fingerprint F0, the 1st user label Lu1, and the 2nd user label Lu2 The original copyright label L0, the original copyright label fingerprint F0, the 1st user label Lu1, the 2nd user label Lu2, and the 3rd user label Lu3 are shown, and distribution of the 2nd private key Ks2 and the 3rd private key Ks3 is required of the data control center Cd.

[0064] (11) The data control center Cd of which distribution of the 2nd private key Ks2 and the 3rd private key Ks3 was required checks whether the original copyright label L0, the 1st user label Lu1, and the 2nd user label Lu2 are just with the original copyright label fingerprint F0. When it is checked that the 2nd user label Lu2 is just, the data control center Cd registers the 3rd user label Lu3, enciphers respectively the 3rd private key Ks3 made to correspond to the 2nd private key Ks2 and the 3rd user label Lu3 corresponding to the 2nd user label Lu2 using the 3rd user's U3 public key Kb3, and is Cks2kb3=E (Ks2, Kb3).

Cks3kb3=E(Ks3,Kb3)

2nd private key Cksof encryption2kb3 and 3rd private key Cksof encryption3kb3 are distributed among the 3rd user U3.

[0065] (12) The 3rd user U3 among whom 2nd private key Cksof encryption2kb3 and 3rd private key Cksof encryption3kb3 were distributed decodes 2nd private key Cksof encryption2kb3, and 3rd private key Cksof encryption3kb3 using the 3rd user's U3 exclusive key Kv3, and is Ks2=D (Cks2 kb3, Kv3).

Ks3=D(Cks3kb3,Kv3)

Encryption original paper crop data Cm0ks2 is decoded using the 2nd decoded private key Ks2, and it is M0=D (Cm0 ks2, Ks2).

The decoded original paper crop data M0 are used.

[0066] In saving and copying the original paper crop data M0 In enciphering using the 3rd decoded private key Ks3, saving and copying encryption original paper crop data Cm0ks3 and transmitting the original paper crop data M0 to the 4th user U4 It enciphers using the 3rd decoded private key Ks3, and encryption original paper crop data Cm0ks3 is transmitted to the 4th user U4 with the original copyright label L0, the 1st user label Lu1, the 2nd user label Lu2, and the 3rd user label Lu3. Henceforth, the same actuation is repeated.

[0067] Drawing 8 explains the 2nd example sent apart from the key used in order that the key used in order to encipher the [2nd example] work data may decrypt work data. In addition, since

the relation of the handling of the key in this 2nd example, the original paper author, an information provider, and a user and the handling of a label are the same as that of the case of the 1st example, explaining again omits them.
[0068] (1) The original paper author A presents the original copyright label L0, and demands distribution of the original private key Ks0 of the data control center Cd.
[0069] (2) The data control center Cd of which distribution of the original private key Ks0 was required creates the original copyright label fingerprint F0 from the original copyright label L0, enciphers the original private key Ks0 to which the original copyright label L0 was made equivalent with the original copyright label L0 using the original paper author's A public key Kba, and is Cks0 kba=E (Ks0, Kba).
Encryption Hara private key Cks0kba is distributed among the original paper author A.
[0070] (3) The original paper author A among whom encryption Hara private key Cks0kba was distributed decodes encryption Hara private key Cks0kba using the original paper author's A exclusive key Kva, and is Ks0=D (Cks0 kba, Kva).
The original paper crop data M0 are enciphered using the decoded original private key Ks0, and it is Cm0ks0=E (M0, Ks0).
Encryption original paper crop data Cm0ks0, the original copyright label L0, and the original copyright label fingerprint F0 are transmitted to the 1st user U1.
[0071] (4) The 1st user U1 to whom encryption original paper crop data Cm0ks0, the original copyright label L0, and the original copyright label fingerprint F0 were transmitted presents the original copyright label L0, the original copyright label fingerprint F0, and the 1st user label Lu1, and demands distribution of the original private key Ks0 of the data control center Cd.
[0072] (5) The data control center Cd of which distribution of the original private key Ks0 was required enciphers the original private key Ks0 corresponding to the original copyright label L0 using the 1st user's U1 public key Kb1 while it checks the justification of the shown original copyright label L0 with the original copyright label fingerprint F0 and registers the 1st user label Lu1, and it is Cks0kb1=E (Ks0, Kb1).
Encryption Hara private key Cks0kb1 is distributed to the 1st user U1.
[0073] (6) The 1st user U1 to whom encryption Hara private key Cks0kb1 was distributed decodes encryption Hara private key Ck0kb1 using the 1st user's U1 exclusive key Kv1, and is Ks0=D (Cks0 kb1, Kv1).
Encryption original paper crop data Cm0ks0 is decoded using the decoded original private key Ks0, and it is M0=D (M0, Ks0).
The decoded original paper crop data M0 are used.
[0074] (7) In saving and copying the original paper crop data M0, the original copyright label L0, the original copyright label fingerprint F0, and the 1st user label Lu1 are shown again, and it requires distribution of the 1st private key Ks1 of the data control center Cd.
[0075] (8) The data control center Cd of which distribution of the 1st private key Ks1 was required enciphers the 1st private key Ks1 which checked the justification of the 1st shown user label Lu1 with the original copyright label fingerprint F0, and was made to correspond to the 1st registered user label Lu1 using the 1st user's U1 public key Kb1, and is Cks1kb1=E (Ks1, Kb1).
1st private key Cksof encryption1kb1 is distributed to the 1st user U1.
[0076] (9) The 1st user U1 to whom 1st private key Cksof encryption1kb1 was distributed decodes 1st private key Cksof encryption1kb1 using the 1st user's U1 exclusive key Kv1, and is Ks1=D (Cks1 kb1, Kv1).
It enciphers using the 1st private key Ks1 which had the original paper crop data M0 decoded, and is Cm0ks1=E (M0, Ks1).
In saving and copying as encryption original paper crop data Cm0ks1 and transmitting the original paper crop data M0 to the 2nd user U2, it enciphers using the 1st decoded private key Ks1, and transmits as encryption original paper crop data Cm0ks1 with the original copyright label L0, the original copyright label fingerprint F0, and the 1st user label Lu1.
[0077] (10) The 2nd user U2 to whom encryption original paper crop data Cm0ks1, the original copyright label L0, the original copyright label fingerprint F0, and the 1st user label Lu1 were transmitted presents the original copyright label L0, the original copyright label fingerprint F0,

the 1st user label Lu1, and the 2nd user label Lu2, and demands distribution of the 1st private key Ks1 of the data control center Cd.
[0078] (11) The data control center Cd of which distribution of the 1st private key Ks1 was required checks the justification of the original copyright label L0 and the 1st user label Lu1 with the original copyright label fingerprint F0. When it is checked that the 1st user label Lu1 is just, the data control center Cd registers the 2nd user label Lu2, enciphers respectively the 1st private key Ks1 corresponding to the 1st user label Lu1 using the 2nd user's public key Kb2, and is Cks1kb2=E (Ks1, Kb2).
1st private key Cksof encryption1kb2 is distributed among the 2nd user U2.
[0079] (12) The 2nd user U2 among whom 1st private key Cksof encryption1kb2 was distributed decodes 1st private key Cksof encryption1kb2 using the 2nd user's U2 exclusive key Kv2, and is Ks1=D (Cks1 kb2, Kv2).
Encryption original paper crop data Cm0ks1 is decoded using the 1st decoded private key Ks1, and it is M0=D (Cm0 ks1, Ks1).
The decoded original paper crop data M0 are used.
[0080] (13) In saving and copying the original paper crop data M0, the original copyright label L0, the original copyright label fingerprint F0, the 1st user label Lu1, and the 2nd user label Lu2 are shown again, and it requires distribution of the 2nd private key Ks2 of the data control center Cd.
[0081] (14) The data control center Cd of which distribution of the 2nd private key Ks2 was required enciphers the 2nd private key Ks2 which checked the justification of the 2nd shown user label Lu2 with the original copyright label fingerprint F0, and was made to correspond to the 2nd registered user label Lu2 using the 2nd user's U2 public key Kb2, and is Cks2kb2=E (Ks2, Kb2).
2nd private key Cksof encryption2kb2 is distributed to the 2nd user U2.
[0082] (15) The 2nd user U2 to whom 2nd private key Cksof encryption2kb2 was distributed decodes 2nd private key Cksof encryption2kb2 using the 2nd user's U2 exclusive key Kv2, and is Ks2=D (Cks2 kb2, Kv2).
It enciphers using the 2nd private key Ks2 which had the original paper crop data M0 decoded, and is Cm0ks2=E (M0, Ks2).
In saving and copying as encryption original paper crop data Cm0ks2 and transmitting the original paper crop data M0 to the 3rd user U3, it enciphers using the 2nd decoded private key Ks2, and transmits to the 3rd user U3 as encryption original paper crop data Cm0ks2 with the original copyright label L0, the original copyright label fingerprint F0, the 1st user label Lu1, and the 2nd user label Lu2.
[0083] (16) The 3rd user U3 to whom encryption original paper crop data Cm0ks2 was transmitted with the original copyright label L0, the original copyright label fingerprint F0, the 1st user label Lu1, and the 2nd user label Lu2 presents the original copyright label L0, the original copyright label fingerprint F0, the 1st user label Lu1, the 2nd user label Lu2, and the 3rd user label Lu3, and demands distribution of the 2nd private key Ks2 of the data control center Cd.
[0084] (17) The data control center Cd of which distribution of the 2nd private key Ks2 was required checks whether the original copyright label L0, the 1st user label Lu1, and the 2nd user label Lu2 are just with the original copyright label fingerprint F0. When it is checked that the 2nd user label Lu2 is just, the data control center Cd registers the 3rd user label Lu3, enciphers the 2nd private key Ks2 corresponding to the 2nd user label Lu2 using the 3rd user's U3 public key Kb3, and is Cks2kb3=E (Ks2, Kb3).
2nd private key Cksof encryption2kb3 is distributed among the 3rd user U3.
[0085] (18) The 3rd user U3 among whom 2nd private key Cksof encryption2kb3 was distributed decodes 2nd private key Cksof encryption2kb3 using the 3rd user's U3 exclusive key Kv3, and is Ks2=D (Cks2 kb3, Kv3).
Encryption original paper crop data Cm0ks2 is decoded using the 2nd decoded private key Ks2, and it is M0=D (Cm0 ks2, Ks2).
The decoded original paper crop data M0 are used.
[0086] (19) In saving and copying the original paper crop data M0, the original copyright label L0,

the original copyright label fingerprint F0, the 1st user label Lu1, the 2nd user label Lu2, and the 3rd user label Lu3 are shown again, and it requires distribution of the 3rd private key Ks3 of the data control center Cd.
[0087] (20) The data control center Cd of which distribution of the 3rd private key Ks3 was required enciphers the 3rd private key Ks3 which checked the justification of the 3rd shown user label Lu3 with the original copyright label fingerprint F0, and was made to correspond to the 3rd registered user label Lu3 using the 3rd user's U3 public key Kb3, and is Cks3kb3=E (Ks3, Kb3).
3rd private key Cksof encryption3kb3 is distributed to the 3rd user U3.
[0088] (21) The 3rd user U3 to whom 3rd private key Cksof encryption3kb3 was distributed decodes 3rd private key Cksof encryption3kb3 using the 3rd user's U3 exclusive key Kv3, and is Ks3=D (Cks3 kb3, Kv3).
It enciphers using the 3rd private key Ks3 which had the original paper crop data M0 decoded, and is Cm0ks3=E (M0, Ks3).
In saving and copying as encryption original paper crop data Cm0ks3 and transmitting the original paper crop data M0 to the 4th user U4 It enciphers using the 3rd decoded private key Ks3, and transmits to the 4th user U4 as encryption original paper crop data Cm0ks3 with the original copyright label L0, the original copyright label fingerprint F0, the 1st user label Lu1, the 2nd user label Lu2, and the 3rd user label Lu3. Henceforth, the same actuation is repeated.
[0089] Since only the key required for use of work data for decode is distributed first in the case of this example, actuation is simplified for the user who does not perform preservation of work data, a copy, or a transfer. In addition, it is also possible to constitute so that the key for re-codes may make the key for decode in the key for re-codes and the system distributed separately live together in one system, may choose suitably like the 1st example like the key for decode, the system by which it is distributed to coincidence, and the 2nd example and it may use.
[0090] The [3rd example] user processes one original paper crop data, and explains the 3rd example transmitted to the next user by drawing 9 and drawing 10 . Processing of a data work is performed by editing original paper crop data using the processing tool which is an application program, and the information and the contents data of processing of the used original paper crop data and the used processing tool can express the processing work data obtained by processing. That is, when the processing tool is owned, it is possible by original paper crop data and the contents data of processing coming to hand to reproduce processing work data.
[0091] Processing of digital data is explained. Since processing of digital data is made by adding an alteration to original data using the program for processing (processing tool), processing data are reproduced by specifying original data, a processing tool, and the contents data of processing (processing scenario). In other words, if original data, a processing tool, and a processing scenario are not specified, reappearance of processing data is impossible.
[0092] In creating new data with single original data When changing the original data A and obtaining processing data "A'", and a user adds Data X to the original data A and processing data "A+X" are obtained, the original data A — the original data elements A1 and A2 and A3, when dividing into ..., changing an array like A3, and A2 and A1 and obtaining processing data "A"" the original data A — the original data elements A1 and A2 and A3 ... dividing — a primary user's data XX1, and X2 and X3 — it may divide into ..., these may be arranged and processing data "A1+X1+A2+X2+A3+X3 ..." may be obtained In these cases, division of the alteration of original data, array modification of original data, the combination of original data and user data, and original data and combination ** with user data need to be respectively set as the object of secondary copyright, and need to protect such secondary copyrights. In addition, it cannot be overemphasized that a user's original copyright exists in the data X which the user added.
[0093] In creating new data by combining two or more original data the original data A, B, and C, when obtaining processing data "A+B+C ...", combining ... simply the original data A, B, and C, when a user adds Data X to ... and it obtains processing data "A+X" the original data A, B, and C ... the original data elements A1 and A2 and A3 ..., B1, B-2, B3, ..., C1, and C2 and C3 ... dividing — combining — an array — changing — processing data — "— A1+B1+C1+ ... +A2+B-2+C2+ ... +A3+B3+C3+ ... ", when obtaining An array is changed combining ... the original data A,

B, and C ... the original data elements A1 and A2 and A3 ..., B1, B-2, B3, ..., C1, and C2 and C3 ... dividing -- a user's data X1, X2, and X3 -- processing data -- "-- A1+B1+C1+X1+ ... +A2+B-2+C2+X2+ ... +A3+B3+C3+X3+ ... " -- it may obtain Also in these cases, combination ** of two or more original data with which it was divided and array-changed and the combination of two or more original data, the combination of two or more original data and user data, and two or more original data were divided, and user data needs to be respectively set as the object of 2nd order-copyright, and needs to protect such 2nd order-copyrights. moreover, the data X1, X2, and X3 which the user added -- it cannot be overemphasized that a user's original copyright exists in ...

[0094] The example of technique which creates the new data D using two or more original data A, B, and C was shown in drawing 9 . This technique processes data by the cut & paste technique which extracts Elements a, b, and c from the original data A, B, and C (cut), sticks the extracted elements a, b, and c, and compounds one (paste) data D.

[0095] In addition, there is a data link technique to which two or more data objects are made to link. This data link technique prepares the ObjectLink section in the slot of the pad (pad) which is a data object, and makes objects link with other pads and the slot connection (slot connection) technique made to link by this slot. Thus, the interrelation of two or more linked objects can be expressed as a tree structure, and the deletion or the addition of an object of it is attained using the tree structure expressed further.

[0096] By the way, although it is clear that original data and user data are data Division of division of the alteration of the original data which are the processing process of data, array modification of original data, the combination of original data and user data, and original data and combination with user data, the combination of two or more original data, the combination of two or more original data and user data, and two or more original data And the combination of two or more original data which were array-changed and were divided, and user data is also the data itself.

[0097] If it notes that the processing scenario of the data which are arrangement relation, a processing procedure, etc. of original data is also data, it will become possible to protect by managing the copyright of the user about processing process data in addition to the copyright of the user about original copyright and user data of the original paper author concerning original data in the secondary copyright about processing data.

[0098] That is, the copyright of processing data is manageable with original data by constituting processing data from original data, user data, and a processing scenario, and managing these original data, user data, and a processing scenario. In addition, if the program for processing used in processing of data in this case is also required, it will consider as the administration object of a data management system.

[0099] Although processing of this data can also process original data using the processing program corresponding to that original data, if original data are dealt with as object-oriented software which attracts attention recently, easier processing and better data copyright management can be performed. Furthermore, if agent-oriented software is adopted spontaneously, a user can compound data, without taking great pains.

[0100] Agent-oriented software is a program which has autonomy, adaptability, and cooperativeness, and even if it does not direct all work habits concretely like the conventional software, it can meet the demand of a user only based on general directions of a user according to a special feature with its autonomy, adaptability, and cooperativeness. a database or copyright management center side can know a user database use inclination , and fine copyright management perform by incorporate this agent program into the fundamental system of a data copyright managerial system , make a user database use gestalt supervise , and constitute so that the information which contain a use data detail , accounting information , etc. using the meter ring function user terminal equipment be equipped with a function be collect by the database or copyright management center side . Therefore, an agent program and data are also set as the object of protection of copyrights, and it is similarly enciphered as original data.

[0101] In the 3rd example shown in drawing 10 , what added the processing scenario to the copyright label in the 1st example and the 2nd example which were shown previously is treated like a "processing label" and the copyright label in a call and the 1st example. In addition, since

the relation of the handling of the key in this 3rd example, the original paper author, an information provider, and a user and the handling of a label are the same as that of the case of the 1st example, what is explained again is omitted.

[0102] (1) The original paper author A presents the original copyright label L0, and demands distribution of the original private key Ks0 of the data control center Cd.

[0103] (2) The data control center Cd of which distribution of the original private key Ks0 was required enciphers the original private key Ks0 to which the original copyright label L0 was made equivalent using the original paper author's A public key Kba with the original copyright label L0, and is Cds0 kba=E (Ks0, Kba).

Encryption Hara private key Cks0kba is distributed among the original paper author A.

[0104] Algorithms, such as MD5, are used for the data control center Cd for the original copyright label L0 at this time, it performs ** at it to 16 bytes of an one direction hash, for example, amount of data, creates the Hara copyright label fingerprint F0, and distributes it to the original paper author A. This electronic fingerprint is created about each processing work, whenever original paper crops or processing is performed and a processing work is obtained, and it is transmitted with a work.

[0105] (3) The original paper author A among whom encryption Hara private key Cks0kba was distributed decodes encryption Hara private key Cks0kba using the original paper author's A exclusive key Kva, and is Ks0=D (Cks0 kba, Kva).

The original paper crop data M0 are enciphered using the decoded original private key Ks0, and it is Cm0ks0=E (M0, Ks0).

Encryption original paper crop data Cm0ks0, the original copyright label L0, and the original copyright label fingerprint F0 are transmitted to the 1st user U1.

[0106] (4) The 1st user U1 to whom encryption original paper crop data Cm0ks0, the original copyright label L0, and the original copyright label fingerprint F0 were transmitted presents the original copyright label L0, the original copyright label fingerprint F0, and the 1st user label Lu1, and demands distribution of the original private key Ks0 of the data control center Cd. [0107] (5) The data control center Cd of which distribution of the original private key Ks0 was required enciphers the original private key Ks0 corresponding to the original copyright label L0 using the 1st user's U1 public key Kb1 while it checks the justification of the shown original copyright label L0 with the original copyright label fingerprint F0 and registers the 1st user label Lu1, and it is Cks0kb1=E (Ks0, Kb1).

Encryption Hara private key Cks0kb1 is distributed to the 1st user U1.

[0108] (6) The 1st user U1 to whom encryption Hara private key Cks0kb1 was distributed decodes encryption Hara private key Ck0kb1 using the 1st user's U1 exclusive key Kv1, and is Ks0=D (Cks0 kb1, Kv1).

Encryption original paper crop data Cm0ks0 is decoded using the decoded original private key Ks0, and it is M0=D (M0, Ks0).

The decoded original paper crop data M0 are processed using a processing tool, and the processing work data Me1 are obtained.

[0109] Thus, the copyright of the original paper author who created original paper crops with the copyright of the 1st user who processed data also exists in the obtained processing work data Me1. The copyright of the original paper author about the original paper crop data M0 with the original private key Ks0 to which the registered original copyright label L0, and the original copyright label fingerprint F0 and the original copyright label L0 were made equivalent, and the 1st private key Ks1 made to correspond to the 1st user label Lu1 and the 1st user label Lu1 Although it can protect, since the key which enciphers the processing work data Me1 is not prepared, the secondary copyright of the 1st user about the processing work data Me1 is not in the condition of still being protected.

[0110] (7) In order to protect the secondary copyright of the 1st user about the processing work data Me1, use the 1st user label which is the author of a processing work, and its electronic fingerprint in the 3rd example. If its 1st user label is regood since the information and the contents data of processing of the used original paper crop data and the used processing tool can express a processing work as explained above, these information and data will be entered in the 1st processing label Le1. Furthermore, for the secondary protection of

copyrights in future circulation processes, a user U1 shows the data control center Cd the 1st processing label Le1, and registration of a user's U1 secondary copyright is performed by this.
[0111] (8) The data control center Cd shown the 1st processing label Le1 While checking the justification of the shown original copyright label L0 with the original copyright label fingerprint F0 and registering the 1st processing label Le1 The electronic fingerprint F1 of the 1st processing label Le1 is created, the 1st processing private key Kse1 to which the 1st processing label Le1 was made equivalent is enciphered with the public key Kb1 of the 1st user U1 of a data control center, and it is Ckse1kb1=E (Kse1, Kb1).
With the electronic fingerprint Fe1 of the 1st processing label Le1, 1st processing private key Ckseof encryption1kb1 is sent to the 1st user U1.
[0112] (9) The 1st user U1 to whom the electronic fingerprint Fe1 of 1st processing private key Ckseof encryption1kb1 and the 1st processing copyright label Le1 was distributed decodes 1st processing private key Ckseof encryption1kb1 using the 1st user's U1 exclusive key Kv1, and is Kse1=D (Ckse1 kb1, Kv1).
The 1st processing work data Me1 are enciphered using the decoded 1st processing key Kse1, and it is Cme1=E (Me1, Kse1).
With the electronic fingerprint Fe1 of the 1st processing copyright label Le1 and the 1st processing copyright label Le1, the 1st processing work data Cme1 of encryption are transmitted to the 2nd user U1. Henceforth, the same actuation is repeated.
[0113] In the 3rd example, although only the electronic fingerprint Fe1 of the 1st processing copyright label Le1 and the 1st processing copyright label Le1 is transmitted with the 1st processing work data Cme1 of encryption at the time of a processing data transfer, it can also constitute so that other labels and electronic fingerprints may also be transmitted to coincidence. Although carried out like [although processing performed using two or more work data as shown in drawing 7 has the complicated part actuation with many work data] the case of processing using single data, it abbreviates to explanation not becoming redundancy.
[0114] In the system of the 1st example explained above, the 2nd example, and the 3rd example, work data are enciphered using the private key and the private key for re-encryption used for the private key for decode, and preservation, a copy and a transfer is distributed by the data control center based on the user label which the user presented.
[0115] Since all are beforehand enciphered with the user public key with which the data control center attested justification, these private keys for decode and the private key for re-encryption will have received authentication of a data control center indirectly. Moreover, since it is used in order that these private keys may encipher the work data transmitted, authentication of the data control center to the work data finally transmitted will also be performed. Since the authentication by this data control center is absolute, it is a hierarchical authentication system represented by PEM.
[0116] On the other hand, since between users is transmitted without transmitting the work data itself to a data control center, it can be said that the authentication performed in the process is a horizontal dispersion mold authentication system represented by PGP. Thus, the authentication system which combines the features that the dependability of a hierarchical authentication system is high, and the features that the treatment of a horizontal dispersion mold authentication system is simple, by the system of this example is realized.
[0117] Moreover, all the contents of the action of the user using work data and the action are grasped in the data control center by the user label which the user presented. and — since use including processing of a work is altogether performed via a data control center — him, each user, — while a check is ensured, the contents of work data and certification of hysteresis are performed by checking the contents of the action, and progress. When this contents certification is applied to electronic commerce etc., it is possible to carry out the certification of the contents of dealings by the data control center, i.e., "electronic authentication." moreover, a user label — or the case where the digital signature is made the processing label — a user label — or if a computer virus invades into a processing label, the data of a label will change and, as a result, a hash value will change. Therefore, invasion of a computer virus is detectable by verifying a digital signature. the hash value which changed when hash value-ization was performed, even if it did not perform a digital signature — a user label — or since

the processing label is invalid, invasion of a computer virus is detectable.
[0118] In the case of the distributed object system represented by the [4th example] license network system, use of the network computer which does not have not a computer but the data storage equipment of the former which has mass data storage equipment, but performs only I/O of data and processing of data is taken into consideration. Furthermore, using the network computer like a terminal unit of a large-sized computer which does not have even a data processor but has only the I/O function of data is also taken into consideration. Since such a network computer does not have data storage equipment, it cannot save or copy work data.
[0119] Next, although an applicable example is explained also to the network computer which does not have data storage equipment used by such distributed object system, this example is being able to apply naturally also to the computer which has usual data storage equipment.
[0120] In order to restrict unauthorized use of a work to protecting data copyright, it is necessary to use a certain code technique. In the 1st example, the 2nd example, and the 3rd example which were explained until now, in order to protect the copyright in the system for the computer which has usual data storage equipment, the label which is not enciphered as a key for using the enciphered work data and work data is used. On the other hand, it sets to the system for the network computer which has only the function like a terminal unit, and since work data are not saved, copied or transmitted, it is not necessary to encipher work data.
[0121] As the 3rd example explained, processing of a data work is performed by changing original paper crop data using a processing tool, and the information and the processing scenario of the used original paper crop data and the used processing tool can express the processing work data obtained by processing. Also when processing work data are created using the work data of the database which is the same also about a distributed object system as for this, and exists on a distributed object system Processing work data are reproducible by specifying the information and the processing scenario of the used database, the used original paper crop data, and the used processing tool. Even if this is the case where two or more work data which came to hand from a single database or two or more single databases are used, it is the same.
[0122] Drawing 11 explains the 4th example. In this example, the original copyright person and information provider (IP) which hold work data are distinguished from the user who does not hold work data, and are arranged with a data control center etc. at a network side. A public key and an exclusive key are used in the system of this example. in addition — the time of original paper crop data being transmitted to a user — an insurance sake — original paper crop data — a private key — or it is enciphered using the public key of the destination.
[0123] Although the 1st user U1 looks for work data and collects required work data using a network, broadcast, or a record medium, even when the collected work data stop at being saved in 1st order on a user's U1 memory and data storage equipments, such as a hard disk drive (HDD), are contained in a user's U1 equipment, work data are not saved to data storage equipment. In order not to save work data, when preservation tends to be performed, prohibition of preservation of work data is performed by performing destruction of the work data on memory, modification of the data header on memory, and one direction hash value-ization of data, and making a change to the preservation impossible file name of a file name etc. Although the data storage prohibition program built in the program part of the work data which have object structure can also perform prohibition of preservation, advanced dependability is acquired by being carried out by the whole system or the operating system (OS) in connection with a user's equipment.
[0124] The 4th example explains the case where two or more work data are used. (1) (2) Although the 1st user U1 shows a data control center the 1st user label Lu1, original paper crop data M0i (i= 1, 2, 3 ...) is collected from the library of data of the information provider IP in a system and the processing tool Pe comes to hand At this time, it is enciphered using the 1st user's U1 public key Kb1, and original paper crop data M0i and the processing tool Pe are
Cm0ikb1=E (M0 i, Kb1).
Cpekb1=E(Pe,Kb1)
Encryption original paper crop data Cm0ikb1 and the encryption processing tool Cpekb1 are

distributed among the 1st user U1. In addition, by referring to the 1st user label Lu1 at this time, the use situation of original paper crop data M0i and the processing tool Pe is also recorded on a data control center, and is used for accounting.

[0125] (3) The 1st user U1 to whom encryption original paper crop data Cm0ikb1 and the encryption processing tool Cpekb1 were distributed decodes encryption original paper crop data Cm0ikb1 and the encryption processing tool Cpekb1 which were distributed using the 1st user's U1 exclusive key Kv1, and is M0 i=D (Cm0 ikb1, Kv1).

Pe=D(Cpekb1,Kv1)

Original paper crop data M0i which carried out and was decoded using the decoded processing tool Pe is processed, and 1st processing work data M1i (i= 1, 2, 3 ...) is obtained.

[0126] (4) The 1st user U1 who got 1st processing work data M1i enciphers 1st scenario S1i which is processing data about 1st processing work data M1i with the public key Kbc of a data control center, and is Cs1 ikbc=E (S1 i, Kbc).

With the 1st user label Lu1, 1st scenario Csof encryption1ikbc is shown to the data control center Cd, and registration of a user's U1 secondary copyright is performed by this.

[0127] (5) The data control center Cd shown 1st scenario Csof encryption1ikbc decodes 1st scenario Csof encryption1ikbc using the exclusive key Kvc of the data control center Cd, and is S1 i=D (Cs1ikbc, Kvc).

The 1st processing label Le1 is created based on the 1st user's U1 shown user label, and decoded 1st processing scenario S1i, it is kept in the data control center Cd, the 1st processing label Le1 is enciphered using the 1st user's U1 public key Kb1, and it is Cle1kb1=E (Lei, Kb1).

1st processing label Cleof encryption1kb1 is transmitted to the 1st user U1.

[0128] (6) The 1st user U1 to whom 1st processing label Cleof encryption1kb1 was transmitted decodes 1st processing label Cleof encryption1kb1 using the 1st user's U1 exclusive key Kv1, and is Le1=D (Cle1 kb1, Kv1).

The decoded 1st processing label Le1 is enciphered using the 2nd user's U2 public key Kb2, and it is Cle1kb2=E (Le1, Kb2).

Although 1st processing label Cleof encryption1kb2 is transmitted to the 2nd user U2, 1st processing work data M1i or the 1st processing work data of encryption is not transmitted to the 2nd user U2.

[0129] When the 1st user's U1 computer has data storage equipment, collection work data or processing data may be saved to data storage equipment, but in order to prevent preservation, a copy, and a transfer, prohibition of above-mentioned preservation is performed. In addition, in this case, instead of 1st processing label Cleof encryption1kb2, the electronic fingerprint F1 which formed the 1st processing label into the one direction hash value can also be used, and a transfer of the simplified processing label with telephone voice is attained by doing in this way.

[0130] (7) The 2nd user U2 to whom 1st processing label Cleof encryption1kb2 was transmitted decodes transmitted 1st processing label Cleof encryption1kb2 using the 2nd user's U2 exclusive key Kv2, and is Le1=D (Cle1 kb2, Kv2).

The 1st processing label Le1 is enciphered using the 2nd user's U2 exclusive key Kv2, and it is Cle1kv2=E (Le1, Kv2).

encryption 1st — processing label Cle1kv2 is shown to the data control center Cd with the 2nd user label Lu2.

[0131] (8) encryption 1st — the encryption 1st shown the data control center Cd shown processing label Cle1kv2 and the 2nd user label Lu2 — processing label Cle1kv2 — the 2nd user's U2 public key Kb2 — using — decoding — Le1=D (Cle1 kv2, Kb2)

Original paper crop data M0i indicated by the decoded 1st processing label Le1 is collected. original paper crop data M0i is processed based on 1st scenario S1i similarly indicated by the 1st processing label Le1 using the processing tool Pe, and 1st processing work data M1i is reproduced.

[0132] The data control center Cd which reproduced 1st processing work data M1i enciphers 1st processing work data M1i and the processing tool Pe using the 2nd user's U2 public key Kb2, and is Cm1ikb2=E (M1 i, Kb2).

Cpekb2=E(Pe,Kb2)

encryption 1st — processing work data Cm1ikb2 and the encryption processing tool Cpekb2 are transmitted to the 2nd user U2.
[0133] (9) the encryption 1st to which the 2nd user U2 to whom the 1st processing work data Cmof encryption1ikb2 ******** processing tool Cpekb2 was distributed was distributed — work data Cm1ikb2 and the encryption processing tool Cpekb2 — the 2nd user's U2 exclusive key Kv2 — using — decoding — M1 i=D (Cm1 ikb2, Kv2)
Pe=D(Cpekb2,Kv2)
1st processing work data M1i which carried out and was decoded using the decoded processing tool Pe is processed, and 2nd processing work data M2i (i= 1, 2, 3 ...) is obtained.
[0134] (10) The 2nd user U2 who got 2nd processing work data M2i enciphers 2nd scenario S2i which is processing data about 2nd processing work data M2i with the public key Kbc of a data control center, and is Cs2 ikbc=E (S2 i, Kbc).
With the 2nd user label Lu2, 2nd scenario Csof encryption2ikbc is shown to the data control center Cd.
[0135] (11) The data control center Cd shown 2nd scenario Csof encryption2ikbc decodes 2nd scenario Csof encryption2ikbc using the exclusive key Kvc of the data control center Cd, and is S2 i=D (Cs2ikbc, Kvc).
The 2nd processing label Le2 is created based on the 2nd user's U2 shown user label, and decoded 2nd processing scenario S2i, it is kept in the data control center Cd, the 2nd processing label Le2 is enciphered using the 1st user's U2 public key Kb2, and it is Cle2kb2=E (Lei, Kb2).
2nd processing label Cleof encryption2kb2 is transmitted to the 2nd user U2.
[0136] (12) The 2nd user U2 to whom 2nd processing label Cleof encryption2kb2 was transmitted decodes 2nd processing label Cleof encryption2kb2 using the 2nd user's U2 exclusive key Kv2, and is Le2=D (Cle2 kb2, Kv2).
The decoded 2nd processing label Le2 is enciphered using the 3rd user's U3 public key Kb3, and it is Cle2kb3=E (Le2, Kb3).
2nd processing label Cleof encryption2kb3 is transmitted to the 3rd user U3. Henceforth, the same actuation is repeated.
[0137] The management preservation only of the processing label with which the information, the processing scenario, and processed User Information of the information, i.e., the used original—paper crop data, which a user does not save work data but is saved only in the database concerning [a user] processing to a user's information on the other hand, and the processing tool which used were indicated carries out, only this processing label is enciphered, and it is transmitted among users in the 4th example using this distributed object system. Therefore, preservation and being copied or transmitted do not have work data.
[0138] Moreover, only a public key and an exclusive key are used in the system of this example, as for this public key, justification is beforehand attested by the data control center, and since the authentication by this data control center is absolute, it is a hierarchical authentication system represented by PEM. And since the processing label transmitted is beforehand enciphered with the user public key with which the data control center attested justification and it is transmitted, the contents will have the certainty which received authentication of a data control center indirectly. Since between users is transmitted without transmitting this processing label itself to a data control center, it can be said that the authentication performed in that process is a horizontal dispersion mold authentication system represented by PGP. Thus, the authentication system which combines the features that the dependability of a hierarchical authentication system is high, and the features that the treatment of a horizontal dispersion mold authentication system is simple, by the system of this example is realized.
[0139] Moreover, all the contents of the action of the user using work data and the action are grasped in the data control center by the user label which the user presented. and — since use including processing of a work is altogether performed via a data control center — him, each user, — while a check is ensured, the contents of work data and certification of hysteresis are performed by checking the contents of the action, and progress. When this contents certification is applied to electronic commerce etc., it is possible to carry out the certification of the contents of dealings by the data control center, i.e., "electronic authentication."

[0140] furthermore, a user label — or the case where the digital signature is made the processing label — a user label — or if a computer virus invades into a processing label, the data of a label will change and, as a result, a hash value will change. Therefore, invasion of a computer virus is detectable by verifying a digital signature. HASSHUCHI which changed when hash value-ization was performed, even if it did not perform a digital signature — a user label — or since the processing label is invalid, invasion of a computer virus is detectable.
[0141] since [moreover,] all the contents of the action of the user who uses work data also in this example, and the action are grasped in the data control center by the user label which the user presented — any of the above-mentioned charging system — although — it functions effectively.
[0142] Although the example which applies the system of [5th example] this invention to electronic commerce is explained, drawing 12 (a) explains first the fundamental case where all processings are performed through a broker.
(1) User (need person) U peruses Broker's S goods catalog through a network, and makes demands on Broker S for the dealings data Qm, such as an estimate about the order of goods which wishes to purchase, purchase-order form, and settlement-of-accounts information.
[0143] (2) The broker S who received the demand of the dealings data Qm enciphers Demand R and the 1st private key Ks1 of the dealings data Qm made from User U using Manufacturer's (producer) M public key Kbm, and is Crkbm=E (R, Kbm).
Cks1kbm=E(Ks1,Kbm)
the encryption demand Crkbm and encryption 1st — private key Cks1kbm is sent to Manufacturer M.
[0144] (3) the encryption demand Crkbm and encryption 1st — the encryption demand Crkbm to which the manufacturer M to whom private key Cks1kbm was sent was sent, and encryption 1st — private key Cks1kbm — Manufacturer's M exclusive key Kvm — using — decoding — R=D (Crkbm and Kbm)
Ks1=D(Cks1kbm,Kbm)
It enciphers using the 1st private key Ks1 which had the dealings data Qm corresponding to Demand R decoded, and is Cqmks1=E (Qm, Ks1).
The encryption dealings data Cqmks1 are sent to Broker S.
[0145] (4) The broker S to whom the encryption dealings data Cqmks1 were sent decodes the sent encryption dealings data Cqmks1 using the 1st private key Ks1, and is Q=D (Cqks1, Ks1).
The decoded dealings data Qm are again enciphered using the 2nd private key Ks2, and it is Cqmks2=E (Qm, Ks2).
The 2nd private key KS2 is enciphered using a user's public key Kbu, and it is Cks2 kbu=E (Ks2, Kbu).
the encryption dealings data Cqmks2 and encryption 2nd — private key Cks2kbu is sent to User U.
[0146] (5) the encryption dealings data Cqmks2 and encryption 2nd — the user U to whom private key Cks2kbu was sent — encryption 2nd — private key Cks2kbu — User's U exclusive key Kvu — using — decoding — Ks2=D (Cks2 kbu and Kvu)
The encryption dealings data Cqmks2 are decoded using the 2nd decoded private key Ks2, and it is Qm=D (Cqmks2, Ks2).
By writing down the contents of order in the decoded dealings data Qm, data are processed, the purchase order Qu which drew up and drew up the purchase order Qu is enciphered using the 2nd private key Ks2, and it is Cquks2=E (Qu, Ks2).
The encryption purchase order Cquks2 is sent to Broker S.
[0147] (6) The broker S to whom the encryption purchase order Cquks2 was sent decodes the encryption purchase order Cquks2 using the 2nd private key Ks2, and is Qu=D (Cquks2, Ks2).
The decoded purchase order Qu is enciphered using Manufacturer's M public key Kbm, and it is Cqukbm=E (Qu, Kbm).
The encryption purchase order Cqukbm is transmitted to Manufacturer M.
[0148] The manufacturer M to whom the encryption purchase order Cqukbm was transmitted decodes the encryption purchase order Cqukbm using Manufacturer's M exclusive key Kvm, and is Qu=D (Cqukbm, Kvm).

Order-received processing is performed according to the contents of the decoded purchase order Qu.
[0149] Next, drawing 12 (b) explains exceptional processing when a user places an order directly to a manufacturer. case [in addition, / this] it is exceptional — setting — the above-mentioned (4) encryption dealings data Cqmks2 and encryption 2nd — up to the phase where private key Cks2kbu is sent to User U, since it is the same as that of the fundamental case where it is shown in drawing 12 (a), explanation for the second time is omitted, and only a different phase from the case of being fundamental is explained.
[0150] (7) the encryption dealings data Cqmks2 and encryption 2nd — the user U to whom private key Cks2kbu was sent — encryption 2nd — private key Cks2kbu — User's U exclusive key Kvu — using — decoding — Ks2=D (Cks2 kbu and Kvu)
The encryption dealings data Cqmks2 are decoded using the 2nd decoded private key Ks2, and it is Qm=D (Cqmks2, Ks2).
By writing down the contents of order in the decoded dealings data Qm, data are processed, the purchase order Qu which drew up and drew up the purchase order Qu is enciphered using the 2nd private key Ks2, and it is Cquks2=E (Qu, Ks2).
The encryption purchase order Cquks2 is sent to Manufacturer M.
[0151] (8) The manufacturer M to whom the encryption purchase order Cquks2 was sent transmits the encryption purchase order Cquks2 to Vendor S.
[0152] (9) The broker S to whom the encryption purchase order Cquks2 was transmitted decodes the encryption purchase order Cquks2 using the 2nd private key Ks2, and is Qu=D (Cquks2, Ks2).
The decoded purchase order Qu is enciphered using Manufacturer's M public key Kbm, and it is Cqukbm=E (Qu, Kbm).
It transmits to Manufacturer M.
(10) The manufacturer M to whom the encryption purchase order Cqukbm was transmitted decodes the encryption purchase order Cqukbm using Manufacturer's M exclusive key Kvm, and is Qu=D (Cqukbm, Kvm).
Order-received processing is performed according to the contents of the purchase order Qu.
[0153] The goods set as the object of this commercial transaction can also consider the computer software performed through a network in addition to goods as management. In that case, Manufacturer M enciphers using a manufacturer's exclusive key Kvm, and the software P dealt with is Cpkvm=E (P, Kvm).
The encryption software Cpkvm is transmitted to Broker S, Broker S decodes the transmitted encryption software Cpkvm using Manufacturer's M public key Kbm, and it is P=D (Cpkvm, Kbm).
The software P with which Broker S was decoded is enciphered using User's U public key Kbu, and it is Cpkbu=E (P, Kbu).
The encryption software Cpkbu is transmitted to User U, and User U decodes the transmitted encryption software Cpkbu using the exclusive key Kvu.
P=D(Cpkbu,Kvu)
[0154] Furthermore, although distributing for pay the cryptographic key of the encryption software saved to are recording media, such as CD-ROM, is performed, it can consider as the object of a commercial transaction by the same approach as the computer software which also described this cryptographic key here.
[0155] Since all the dealings are performed through a broker when [fundamental] explained by drawing 12 (a), generating of the various failures by a broker being excluded from a dealings process is prevented beforehand. Moreover, when [exceptional] explained by drawing 12 (b), in order for a manufacturer to get to know the contents of the purchase order and to perform order-received processing, it is necessary to transmit an encryption purchase order to a broker and to have you decrypt by the broker. Therefore, in order that a broker may surely participate in a dealings process also in this case, generating of the various failures by a broker being excluded from a dealings process is prevented beforehand similarly. In addition, it is sent independently, and also it can incorporate into dealings data and the private key sent can also be sent.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] The explanatory view of a label.
[Drawing 2] The explanatory view of a label, a data header, and the data body.
[Drawing 3] A label and the explanatory view of a data encryption.
[Drawing 4] The explanatory view of encryption of a data header and the data body.
[Drawing 5] The explanatory view of encryption of a label, a data header, and the data body.
[Drawing 6] The explanatory view of object file encryption.
[Drawing 7] The outline block diagram of the digital data managerial system of the 1st example of this invention.
[Drawing 8] The outline block diagram of the digital data managerial system of the 2nd example of this invention.
[Drawing 9] The explanatory view of the technique which generates one data from two or more data.
[Drawing 10] The outline block diagram of the digital data managerial system of the 3rd example of this invention.
[Drawing 11] The outline block diagram of the digital data managerial system of the 4th example of this invention.
[Drawing 12] The outline block diagram of the digital data managerial system of the 3rd example of this invention.

[Translation done.]